2013 46th Hawaii International Conference on System Sciences

Group Support Systems Research in the Field of Business Information Security; a Practitioners View

Yuri Bobbert
University of Antwerp (UA)
yuri.bobbert@ua.ac.be

Hans Mulder
Antwerp Management School (AMS)
hans.mulder@ua.ac.be

Abstract

This paper describes the application of Group Support Systems (GSS) in the field of Business Information Security Governance (BISG). The focus is on longitudinal small team collaboration – for instance within Boards of Directors (BoD) and groups of experts – with large amounts of items. Apart from this focus on small groups, there is an operational link to the Information Security Management cycle (Plan, Do, Check, Act i.e. ISO27000 norms). This link results for expert and management teams in collaboration on lots of items (e.g. 133 controls or in this case 228 best practices). This paper presents the findings of an initial research phase and presents a comprehensive, thoroughly selected core set of BISG practices to be used by practitioners. It shows how GSS can play a facilitating role in small team collaboration with large amounts of data. It concludes with suggestions for further empirical research into the BISG topic.

1. Introduction

This paper is part of a larger research study in the field of Business Information Security. It focuses on the first phase of selecting, ranking and validating a large amount of BISG practices via GSS. The initial phase consists of a review of academic and practice oriented literature on relevant Governance Practices by a GSS expert panel.

Group Support Systems (GSS) have emerged over the last 15 years. In "*Fifteen Years of GSS in the Field, A Comparison Across Time and National Boundaries"* [1], De Vreede describes the use of GSS as highly efficient, effective and user friendly. In addition, the facilitation of group dynamics adds consistent value to the systematic collection of data. For this type of research a GSS facilitates the effective collection, organization, evaluation, cross impact analysis and reporting of data [2]. GSS is often used either to diverge or to converge the decision making process on a number of items in a single meeting. However, GSS is only rarely applied as a system in which dozens of teams share their knowledge about hundreds of items in a specific domain over a longer period of time [3]. The application of GSS for large scale and longitudinal research has been identified by De Vreede et al [1]. De Vreede et al substantiated their findings with the following case studies:
Boeing Aircraft corporation (USA)
– 654 participants in 82 GSS-sessions (average team size 7.9);
International Business Machines (IBM) (USA)
– 441 participants in 55 GSS-sessions (average team size 8.0);
Nationale Nederlanden (Netherlands)
– 414 participants in 41 GSS-sessions (average team size 10.0).

A recent case study from The Dutch Policy Academy shows 45 GSS-sessions from 2005 to 2011 in which 763 Academy students participated [4]. The average group size was 16.9. Research on GSS shows an average of 8 up to 17 participants per session. Literature indicates in these cases that the number of items to be generated, organized and evaluated ranges from 30 to a maximum of approximately 50 items [4]. The rationale behind the planning and guarding of a limited number of items – which is part of the preparation of the meeting and responsibility of the facilitator is the 'limited' time and 'processing' power of teams with group sizes up to 17 participants. The current research project focusses on smaller groups such as security experts, Boards of Directors and Management Teams. The group size of these teams is often twice to four times smaller than the average group size of 8 to 17 participants.

Focus / expert groups make it possible to elicit views and perceptions from a diverse group of experts [5]. When making use of facilitating functions such as a computer-assisted analysis of qualitative data (CAQDAS), it is essential to respect the GSS ground

1530-1605/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2013.244

rules as researched by Mariëlle den Hengst in 2005. Her research presents an approach to attain valid information for determining the optimum set of facilitation functions and ground rules that have been applied in the current research project [6]. "There is no 'ideal size' for a focus group [7]. "*Focus group sessions can be structured, or unstructured, depending on the purpose of the research. The group discussion is led, and controlled, by a facilitator whose role it is to: stimulate a free-flowing discussion; help members share their experiences; elicit the views of all participants; keep group members on track; and capture responses*." [5] The role of the facilitator is important in order to avoid the "Asch Effect" where certain individuals dominate the group dynamics and therefore the outcome of the discussion [8]. In the GSS field there has been very little work on differences in group size [9]. For the current research project, experts were selected for a qualitative analysis of applicable processes, structures and relational mechanisms that contribute to BISG. Since group size influences the ability of groups to achieve a productive outcome [10], the selection of the right (number of) experts is key to obtaining collective intelligence. The quality of the outcome of the group ought to be better than the individual opinions before the discussion [11]. Inviting the right number of participants with the appropriate kind of expertise is an important step. If their number is too high, there might be too much "noise on the line". Too few participants may result in little qualified data to generalize the opinions of the experts. In practice only a few people are acknowledged as true experts in the field of BISG. Because BISG involves the discussion of multiple domains, the background of the experts has to be multidisciplinary as well in order to have a good interaction in which experts challenge and validate the items and each other's opinions.

Moreover, the number of items to be discussed is an important variable in the set-up of the meeting. Participants discuss comprehensive lists of items and a number of measures are necessary to facilitate this process. One measure to retain attention during the meeting is to introduce a 'carrousel' in which each expert starts with a different list of items to comment on. After this first round, the expert reviews the comments of the expert sitting next to him/her. In doing so, all the other lists of items are reviewed. This measure also speeds up the process of generating unique comments. After all the comments of individual group members have been generated, the group discusses them – guided by the facilitator. Another measure to handle many items is to ask every participant to study the items on the agenda in advance. In doing so, the expert is also able to verify that he/she really is a true expert in the domains that are to be discussed.

In "How to make collaboration work" [12] David Strauss examines how to build consensus and to generalize opinions phase-by-phase with small groups. In the current research project, a phase-by-phase and longitudinal approach to group support systems is adopted in order to provide generalizable results. The researcher will coin this GSS approach as the 'Securimeter'.

2. Background of the research project

In 2009 and 2010 GSS supported research was started in which a core set of Security Management practices was compiled and validated by a group of experts in the field of IT Security Management [12]. The set of Security practices proposed by the group of experts and subsequently validated by organizations, showed a lack of attention to governance practices. These findings are supported by literature [13] [14] [15]. The lack of attention to governance practices is a problem for two reasons: firstly, governance is a necessity for mandating security management [16]. Secondly, security ought to be part of the organizational culture but is not [17] [18]. The aim of this research project is to develop a framework supported by a large-scale and longitudinal group support system to monitor, evaluate and direct business security governance with small teams (e.g. Boards of Directors, Executive Management Teams). The first section of the paper consists of definitions within the BISG topic. The second section deals with a review of recent academic and practice-orientated literature relevant to BISG. A number of experienced security experts were subsequently asked to assess this large amount of data (228 practices). The experts selected, organized and ranked the practices via GSS. The results enabled further examination of the factors influencing Governance Practices. These findings will serve as potential input for developing a framework to monitor, evaluate and direct BISG.

2.1 Defining Business Information Security Governance

There are various ways in which organizations can attain their strategic objectives. Three dimensions are of strategic importance in this respect: Governance, management and operations. In this article, we define

Governance as *"the guidance of a setting in which others can manage effectively*", Management as *"the making of operating decisions"* [19] and the actual Operations as systems in which people and processes produce products and services. These three dimensions need to be harmonized in order to achieve business objectives, aligned with the appropriate risk. Recent ISACA (Information Systems Audit and Control Association) papers on COBIT5 [20] separate Governance from Management. They are viewed as two disciplines encompassing different activities, organizational structures and therefore serving different purposes. In COBIT5, Governance is defined as follows: *"Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options, setting direction through prioritization and decision making, and monitoring performance, compliance, and progress against plans."* In most enterprises, Governance is the responsibility of the Board of Directors under the leadership of the chairperson. In COBIT5, Management is defined as the discipline that *"plans, builds, runs and monitors activities in alignment with the direction set by the Governance body to achieve the enterprise objectives."* [20] In most enterprises, management is the responsibility of the executive management under the leadership of the CEO. Figure 1 shows COBIT5's distinction between Governance and management activities.

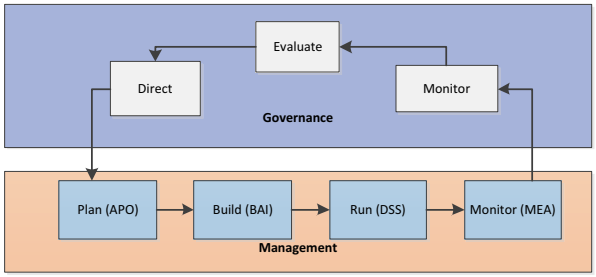

Figure 1 COBIT5 distinction between Governance and Management activities

Basie and Rossow Von Solms are among the few academics who have researched the area of Information Security Governance (ISG). In their study they emphasize that Security Governance ought to be part of Corporate Governance and IT Governance (illustrated in fig. 2) [21]. Their Information Security Governance definition is: *"ISG consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, technologies and compliancy enforcements mechanisms, all working together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people etc.) are maintained at all times"*. The importance of information, technology, people and processes [14] has transformed Information Security (IS) from a technical responsibility into an integral part of the daily business operations called "Business Information Security". Therefore, the following definition for Business Information Security Governance is relevant here; "*Business Information Security Governance (BISG) is an integral part of Corporate Governance exercised by the Board overseeing the definition and implementation of processes, structures and relational mechanisms in the organization that enables confidentiality, integrity and availability (CIA) of the business operations towards all stakeholders"*.

The word integral in this definition refers to the fact that BISG involves multiple disciplines besides IT, e.g. high level accountability on a legal level [21]. 'Exercised by the board' implies that the highest level of the organization is directed towards management and operation. With this definition the researcher aims to incorporate all previous definitions relevant to Governance of Business Information Security. Because the term 'activities' does not cover all the structures, processes and cultural aspects relevant to BIS, the researcher uses the broader terminology of "Practice".

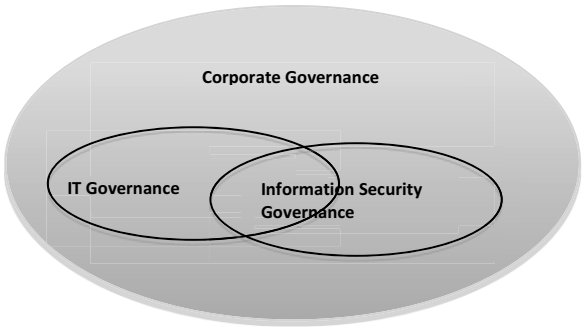

Figure 2 : Information Security Governance positioned by S.H. von Solms & R. von Solms (2009)

2.1 Research Relevance

In the light of Von Solms' analysis of the beneficial effects of the exchange of practices between Corporate Governance practices and Security Governance, research into Corporate Governance

practices is needed. Following the strategic organizational theory of De Wit & Meyer [22], De Haes and Van Grembergen researched "effective" IT governance practices and their ease of implementation [23]. Their Governance practices have been successfully applied into organizations and are therefore also relevant to the aim of this research.

3. Research Method & Findings

3.1 Literature Review

The current research project started with an extensive literature study, capturing all literature on Governance Practices relevant to the topic of Business Information Security Governance. The reviewed governance practices are;

1. Corporate Governance practices;
2. Risk Governance practices;
3. Enterprise Governance of IT practices and
4. Information Security Governance Practices.

1. Approximately 50 best practices from the **Corporate Governance** discipline were examined. The major sources of origin of these practice are: The OECD Principles of Corporate Governance [24]; the Commonwealth Association for Corporate Governance [25]; Internal Control Guidance to Directors, Turnbull report [26]; The Financial Reporting Council (FRC) Combined Code [27], The King Report on Corporate Governance for South Africa [28]; Bank for International Settlements (BIS). Basel principles for enhancing corporate governance [29], Security and Exchange Commission add-ons to SoX, Commission on Public Trust and Private Enterprise 2003. All of them can be found in the Corporate Governance Book (Oxford University Press) which covers all international Corporate Governance codes [30].

2. A major component of practicing good Governance is the **Risk Governance** discipline. Insufficient Risk Governance and management has enormous consequences for all major stakeholders [31]. The judgment and management of IT related risks has become increasingly important to the success of businesses [32]. For the assessment of all relevant Risk Governance practices, the researcher examined literature from: COSO's Enterprise Risk Management Integrated Framework [33]; COSO's "Embracing Enterprise Risk Management": Practical Approaches for Getting Started [34]; COSO's "Where Board of Directors Currently Stand in Executing Their Risk Oversight Responsibilities" [35]; King's Report on Corporate Governance for South Africa [28], and Douglas Hubbard's study on Risk Management Failures. A total of forty Risk Governance Practices were selected.

3. Forty **IT Governance** practices were selected from several sources: IT Governance Institute, "Information Risks: Whose Business Are They?" [36]; De Haes & Van Grembergen's "Practices in IT Governance and Business/IT Alignment" published in ISACA's journal (Information Systems Audit and Control Association); Weil & Ross' "IT Governance" [37] and De Haes & Van Grembergen's book "Implementing Information Technology Governance; Models Practices and Cases" [23] and Van Grembergen's "Strategies for Information Technology Governance" [38].

4. During the selection of the literature, numerous academic and practice oriented sources were investigated, predominantly to judge their appropriateness for ISG practices. The researcher investigated a large number of resources on **Information Security Governance**, because this discipline is the most closely related to Business Information Security Governance (BISG). The researcher investigated sources from an international context to avoid missing out on important developments worldwide; multi sources (Research institutes such as IDC and Gartner) and academic journals and books (from Harvard Business Press, Springer, and Wiley). The research also focused on best practices institutes such as ISACA, ITGI, ISF, SABSA etc., and other communities practicing Security Governance. An examination of highly respected and well established literature sources resulted in a selection of 98 practices. The major literature sources are: the 2004 Corporate Governance Task Force Report of the National Cyber Security Summit [39], chapters "Information Security Governance and Responsibilities of the Board of Directors/Trustees"; De Haes & Van Grembergen's "Practices in IT Governance and Business/IT Alignment" (in ISACA's journal, 2008) [40]; Von Solms's, "The 10 deadly sins of information security management" [40] and other major relevant sources on the BISG topic [41] [42] [43] [44] [45] [14] [21].

The practices that where examined and selected may be potentially applicable for BISG. In order to delete doubles, vaguely articulated practices and so on, a thorough validation of all 228 practices by an expert panel is essential. Before presenting the total of 228 practices to the expert panel, the researcher first structured them by marking them with their origin (source of literature) as well as their discipline

(RG=Risk Governance; CG=Corporate Governance; ITG=IT Governance; ISG=Information Security Governance). In addition, the researcher organized the candidate practices by marking them according to De Wit & Meyer's Strategy Theory [22]: "*Organizational Structures, Processes & Relational Mechanisms"* respectively. In the current research project, the researcher uses a more exhaustive terminology when discussing Relational Mechanisms because the term addresses more than just the culture of an organization such as respect, attitude or behavior. De Wit and Meyer's theory was successfully applied in other studies [46] and was applied by Van Grembergen and De Haes in the development of a framework for the Enterprise Governance of IT. This framework and the three major components for compiling a set of BISG practices are applied in the current research project. During the literature review all 228 practices were marked including marks for Process Contributing Practices (P), Structure Contributing Practices (S) and Relational Mechanisms Practices (RM). The experts were presented with a complete list of 228 practices. They were asked to analyze and investigate this list which was defined as the "Complete List of Governance and Management Practices".

3.2 GSS Expert Panel

In order to organize, assess and rank the practices, a Group Support System (GSS) was used in order to facilitate the expert focus group.

Table 1 Experts panel characteristics

	EXPERTS CHARACTERISTISC AND DISCIPLINES						
EXPERT PROFILE AND TITLE	POSITION	MANAGER	PRACTITIONER	BUSINESS ADVISORY	AUDITOR	CONSULANT	EXPERTISE IN YEARS
BSc RE CISM	Security Officer at Bank	Y	Y	Y	Y	N	>20
BSc CISSP CEH	Security Architect Telco	N	Y	Y	N	Y	>10
MSc RE	Manager at IT Advisory	Y	Y	Y	Y	Y	>15
MSc BSc CISM	Security Consultant	N	Y	Y	Y	Y	>20

Quality is preferred over quantity since the researcher wishes to achieve a thoroughly analyzed and ranked set of practices according to true experts. Four experts were selected according to the following criteria: they have a BA or MA degree in Information Systems, completed with industry certificates i.e. Certified Information Security Manager (CISM); Certified Ethical Hacker (CEH); Register EDP-auditor (CEH). The chosen experts have over 10-year experience in Business Information Security; they are full-time practitioners in Business Information Security and have (had) a link to the strategic management of organizations. These four experts are perfectly situated to select and rank this huge amount of literature data which makes their assessments highly relevant. Due to their multidisciplinary backgrounds (see table 1), their opinions are generalizable across multiple domains and different types of industries. The group size is similar to a Board of Directors or Executive Management Team and will therefore enable us to test on collaboration in small teams with large data sets.

4. GSS Research Data Findings

All 228 practices relevant to the topic of Business Information Security Governance were examined by the four experts via GSS. Because of the time available for assessing and organizing the items, each expert pre-assessed each of the four data sets and passed it back to the group (carrousel concept). Short commentaries were given within GSS to justify the deletion or un-doubling of items. See below for some examples of experts judgments and opinions on certain practices. The practices that are potential candidates for further research are discussed below, as are the practices which received a wide variety of opinions as well as relevant criticisms.

50 practices from the Corporate Governance literature were assessed and organized by experts opinion via GSS. The first and most essential one is the role of the stakeholder:

> *CG P Determine the Role of Stakeholders*. The corporate governance framework should recognize the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises. Source: The OECD Principles of Corporate Governance, 2004, extracted September 24 2011 from www.oecd.org

- The experts commentary on this Corporate Governance practice is that it is a Duplicate to the stakeholder analysis mentioned by numerous other sources. They also comment that this one is focused on financial institutions. One of the experts also commented that the role of the stakeholder is often regulated in laws.

CG RM *Adequate knowledge on the protection of intellectual capital.* Ensure the motivation and protection of intellectual capital intrinsic to the corporation; ensure that there is adequate training in the corporation of management and employees, and a succession plan for senior management (principle 12). Source: Commonwealth Association for Corporate Governance [25].
- The experts commented that the wording of these practices was rather vague. They mentioned that awareness is the key word here. According to the experts, these practices can be assembled under *Creating awareness by adequate knowledge on the protection of intellectual capital*.

CG S *Responsibilities of the Board.* The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders. [24]
- The experts commented that this is a duplicate of other sources mentioning the importance of having a accountable and responsible person at the level of the Board of Directors. One expert said "although I agree that the entire board should take responsibility, not just one man". The expert panel agreed on the replacement of this practice by more specific practices: *Appoint a responsible and accountable board member for risk management and see to it that the company has implemented an effective ongoing process to identify risk, measure its potential impact against a set of assumptions, and then activate what it believes is necessary to proactively manage these risks* [28].

During this research step, the experts concluded that Corporate Governance Practices are often vaguely phrased and therefore it is difficult or even impossible to implement them because organizations do not know how. That is why the researcher asked the experts to rephrase important Governance Practices into more understandable formats. Many of the Corporate Governance practices are a derivative of others so a large number of practice are marked as duplicates. The experts were asked to mark these and they were subsequently deleted, with the facilitator agreeing. All experts pointed out that many of the governance practices they assessed are crucial to the final implementation of good Security Management Practices into operations. They are pre-requisites for any organization.

After the assessment of the Corporate Governance practices the next discipline, Risk Governance was subject for judgment. The assessment of these Risk Governance practices resulted in under mentioned summary of most noticeable findings.

RG P *Aligning risk appetite and strategy*.
Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks [33].
-One of the experts commented that this should be formulated more simply; risk appetite should be aligned with business strategy and accompanying objectives. Determining the organizations risk appetite is stated in most of the Governance academic and practice oriented sources, predominantly because history taught us the importance of doing so (see Enron, MCI Worldcom etc.).
RG RM *BoD understanding of risk philosophy and appetite*. The board should understand the entity's risk philosophy and concur with the entity's risk appetite [34].
- The experts commented that the risk philosophy always needs to be linked to business strategy and therefore to risk appetite. It is important to note here that understanding risk philosophy has more to do with the awareness of the recognition and understanding of risk philosophy at board level and the behavior and attitude towards risks.

A large amount of consensus was reached during this stage of the research. Most of the experts recognized the most relevant Governance Practices. This is acknowledged by the fact that during this step of the research the lowest level of variety is measured in GSS. This is especially the case with the practices "*Determine Roles, Accountabilities and Responsibilities"* and *"Transparency"*.

Numerous Risk Governance Practices again overlap with each other or even other disciplines: for example, Roles and Responsibilities; Stakeholder Identification and identifying events that can threaten business continuity. It is interesting that the Leadership of driving Risk Governance practices is important. COSO mentions this numerous times in several reports [34] [33]. Within Corporate

Governance practices literature, this subject is never mentioned perhaps because it is assumed that leadership is inherent to the personality of any Board Member. Nevertheless, according to the literature, leadership is one of the factors that contributes most to business success or failure [31] [47]. In this case it is an essential finding to take into consideration.

In this next step the researcher assessed the practices within the Enterprise Governance of the IT domain. Since businesses depend more and more on IT, the security of these systems is greatly important. Not only the confidentiality of the information but also the integrity and availability of the information systems are important. This makes the practices from Governance of IT relevant to an examination of Business Information Security Governance. Again, the best candidates and the ones that were discussed most intensely are addressed;

ITG P *IT performance measurement* (e,g, IT balanced score card) [23]
- The experts commented that this could be aligned with the BSC from business units.

ITG P B*oard reviews the risk management approach* for the most important IT-related risks on a regular basis, at least annually [36]
- Experts mentioned that these plans could be integrated into the total of risk management (so IT risks should not be separated).

ITG R *IT leadership* [40]
- Experts pointed to the very high level of this Practice. All of them emphasized that Leadership is always a very important practice, especially at Governance level. In other words, it is important that people "lead by good example".

During this research stage, the experts reach full consensus on the IT Governance practices mentioned above: according to the experts, they are less relevant to the security topic. The main reason for this is that they hugely overlap with the other practices. IT is part of the organization but less integrated than for example risk management (risks arise on multi-levels, such as personnel, finance, safety etc.). Another argument is that IT Governance Practices can be incorporated by rephrasing them into Information Security Governance Practices. In other words, the researcher uses the relevant practices of this research stage and incorporates them into the next stage: assessing and organizing the Information Security Governance Practices.

Finally, organizing Information Security Governance (ISG) Practices was on the agenda of the experts panel session. This practice appears to be most closely related to the topic of Business Information Security Governance. Therefore, it potentially hides the best candidates. The next important step is to have experts assess all of them and make comments if they disagree. It is important to note here that Information Security Governance is not the same as *Business* Information Security Governance. Incorporating the security of the business - and all its related dimensions e.g. risk management - as a whole is of utmost importance to the exact distinction and specification of this domain. The hypothesis that most of the relevant practices for BISG might potentially lie in other disciplines than IT and Security can be proven by the score of the practices. If only ISG practices arise in the ranking, the hypothesis proves to be false. If other Governance disciplines arise, the hypothesis will be confirmed.

Acknowledging *all* relevant Governance practices in selecting the core BISG practices is important, especially because all previous research and literature addresses the necessity of Security management and does not address Governance. Governance is a necessity for mandating security management. Hence, "Good Governance" is essential to mandating it into the efficient operationalizing of security management. An assessment of the ISG practices provides the following findings:

ISG RM *IT Dependency.* Understanding the criticality of information and information security to the organization. [39]
- Experts comment that this practice is vague. "What is there to understand, and especially, how to measure understanding? And by whom?". The experts also mentioned that this practice is relevant since some of the BoD members are not aware of the extent to which their business relies on IT.

ISG RM *Security awareness at level of Board of Directors.* A certain level of awareness about business risks, business critical information, level of information (IT) dependency, kind of threats from outside and inside. [23]
- Experts completely agreed on this practice since organizations nowadays lack adequate knowledge or awareness to enforce appropriate action.

Experts agreed that practices ought to be simple and easy to understand by Board members. Examples are;

ISG *P Do simple risk assessments.* Do simple, subjective risk assessments, and put your efforts into improving security [39].
ISG P *Report simple* (Red-Yellow-Green). Use a simple High-Moderate-Low (Red-Yellow-Green) ranking [39].
ISG RM *Create a measurable security-aware culture* [41].
ISG P *Security maturity assessments.* Determine current BIS maturity level based upon COBIT [42].

In conclusion, it can be stated that, at the end of this step (analysis of and completing of practices per domain), the expert panel team derived a "clean" list of practices from a large amount of (literature) data. Some of the practices were deleted (because they were duplicates) and some were rephrased to avoid misinterpretation in the next research step, ranking the practices on Effectiveness.

4.1 Ranking the GSS Data

The level of effectiveness is the first selection method. A Likert scale was used on which 0 ranks as not effective and 5 ranks as highly effective, mainly because it is our intention to select the best working practices according to experts. In this way this research project can contribute to solving the problem of the low level of security within organizations. These best working practices can later be used as candidates for the next ranking on "Ease of Design and Realization", "Ease of Maintenance" and "Ease of Implementation", also on a scale from 0 to 5. Assessing and ranking all practices over these three dimensions will enable us to determine which practices will work on a management level according to the principles of ISO38500 standard, and can be monitored and evaluated by the Board (Governance level). In consensus with the experts the researcher decided to rank the top practices, measured from 4 and above on effectiveness. In order to compile a list to be judged on these four criteria (1. "Effectiveness", 2. "Ease of Design and Realization", 3. Ease of maintenance and 4. Ease of Implementation) that contributes to the ongoing process according to the ISO 38500 principles. The graph in figure 3 reflects the outcomes of this research phase. It displays the accumulated score on Effectiveness, Ease of Design & Realization, Implementation and Maintenance. This ranking also provides insight into the level of theoretical practices ranked via GSS for practical use. These views of the practitioners on the practical usefulness of the theory in question provides the latter with necessary and meaningful feedback.

5. Framework for BISG Practices

The research question formulated at the beginning of this project - "What is a framework for Business Information Security Governance practices, according to the academic literature on the subject and the views of experts?" - can now be answered in a dual way. Firstly, the framework for Business Information Security Governance consists of all the relevant literature on the topic, which has been examined and elaborated upon throughout this paper. Secondly, this framework consists of three components: structures, processes and relational mechanisms. With the help of the expert panel research, through GSS team collaboration, the researchers organized, ranked and captured the most relevant and effective ones, per component in the theoretical framework (figure 4). This framework can

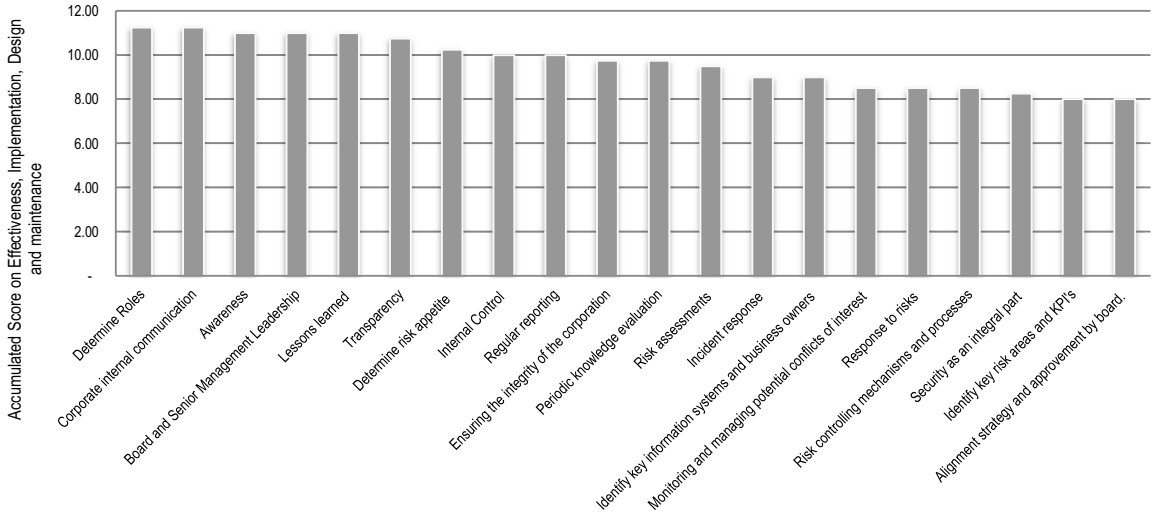

Figure 3 Top 20 Practices for BISG according to the Literature and Experts Validation

serve as a theoretical departure for further research on the basis of the following important questions:

- Which factors influence the acceptance of Governance practices in an organization? These factors include budgets, knowledge, innovation, culture, demographics and so on.
- Do these practices address the major Business Risks inherent to the current security problems?

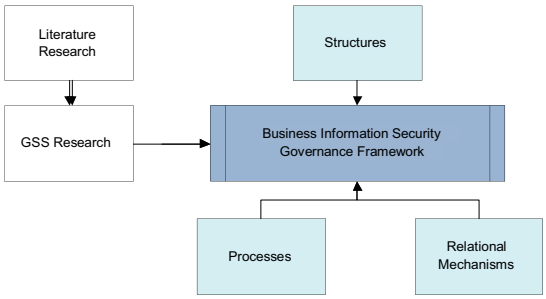

Figure 4 Theoretical Framework for BISG

6. Conclusions and Further Research

This multidisciplinary, multi-layered approach to GSS security research has generated important findings. The hypothesis that other Governance practices than IT and Security would deliver relevant practices for BISG has been confirmed. Half (50%) of the top twenty Governance practices for Business Information Security come from either Corporate Governance or Risk Governance. As a result of our findings, a highly significant core set of Business Information Security Governance and Executive Management practices could be established. In the next phase of this research project, this core set must be tailor-made for specific (organizational) environments by:

1. Analyzing the influencing factors mentioned in the framework paragraph;
2. Testing the acceptance on the part of the executive management of organizations;
3. Investigating whether these practices can be evaluated, directed and monitored, according to ISO38500 Governance within the organization.

In this further research, the researchers present the core set and the influencing factors (i.e. large data sets) to an organization, to small groups of BoD and MT's within this organization. And ask them to participate in the collaboration process as to what works for them and how organizations organize and measure their state per top practice (e.g. roles, risk appetite, incident response) and formulate follow-up actions (monitor, evaluate, direct) in order to maintain a certain level of Business Information Security maturity. This practice oriented research will immediately contribute to organizations since the latter can adopt the core set of governance practices. To form a justified, generalizable and practice oriented opinion on how several organizations and their BoD and MT's adopt and organize BISG, the researcher propose large scale, longitudinal research via this GSS Securimeter method. In this way a socially justified method (due to team collaboration on a large set of pre-defined data (i.e. top 20)) of practical Business Information Security consultancy will "encompass social and adaptable security methods that are rigorously developed along with practice" [48]. The result of this first phase of the research project is the design of a framework to monitor, evaluate and direct business information security governance. According to Hevner's design science research method [49], the next phase will consist of the implementation of the framework in GSS and the testing of the framework in several types of organizations such as critical infrastructure organizations, government institutions and critical data processing organizations over a longer period of time.

References

[1] G. Vreede, D. Vogel, G. Kolfschoten and J. Wien, "Fifteen Years of GSS in the Field: A Comparison Across Time and National Boundaries," in *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)*, 2003.

[2] G. Vreede, J. Boonstra and F. Niederman, "What Is Effective GSS Facilitation? A Qualitative Inquiry Into Participants' Perceptions," in *Proceedings of the 35th Hawaii International Conference on System Sciences*, Delft University of Technology Netherlands, 2002.

[3] Mulder J.B.F. et al., "New Applications of Group Support Systems," *Group Decision and Negotiation, University of Vienna, Austria,* 2005.

[4] Snel, N. "Group Support Systeem: tactisch concept in.," *Opsporing Belicht, Politieacademie,,* Vols. Lectoraat Criminaliteitsbeheersing & Recherchekunde, NL 2011.

[5] R. Newby, G. Soutbar and J. Watson, "Group Support System Approach," *International Small Business Journal,* vol. 21, no. 4, pp. 421-433, 2003.

[6] D. Hengst, "Which facilitation functions are most challenging: A global survey of facilitators," Delft University of Technology, Delft, 2005.

[7] E. Fern, "The Use of Focus Groups for Idea Generation: The effects of Group Size, Acquaintanceship, and Moderator on Reponse Quantity and Quality," *Journal of Marketing Research,* vol. 19, pp. 1-13, 1982.

[8] S. Asch, "Effects of group pressure upon the modification and distortion of judgment.," *In H.Guetzkow (ed.) Groups, leadership and men,* vol. Carnegie Press, Pittsburgh, 1951.

[9] Turoff, M., "Social Decision Support Systems (SDSS)," in *Proceedings of the 35th Hawaii International Conference on System Sciences - 2002*, Hawaii, 2002.

[10] Dennis, A. et al "An experimental investigation of the effects of group size in an electronic meeting environment.," *IEEE Transactions on Systems, Man and Cybernetics,* vol. 20, no. 5, pp. 1049-1057, 1990.

[11] H. T. M. Linstone, The Delphi Method, Techniques and Applications, New Jersey Institute of Technology, 2002.

[12] Y. Bobbert and J. Mulder, "A Research Journey into Maturing the Business Information Security of Mid Market Organizations," International Journal on IT/Business Alignment and Governance, 1(4), US, 2010.

[13] B. Solms, "Corporate Governance and Information Security," Computers and Security, 20 SA 2001

[14] ISACA, "An Introduction to the Business Model for Information Security," ISACA, United States, 2009.

[15] B. v. Solms, "Information Security governance: Cobit or ISO 17799 or Both," Computers & Security, SA 2005.

[16] B. v. Solms and S. Posthumus, "A framework for the governance of information security," Elsevier SA 2004.

[17] B. Von Solms and R. Von Solms, "From Policies to Culture*," Computers & Security 23*, South Africa, 2004.

[18] B. Von Solms and R. Von Solms, "The 10 deadly sins of information security management," Elsevier; Computers & Security 23 (371-376), South Africa, 2004.

[19] A. Sohal and P. Fitzpatrick, "IT governance and management in large Australian organisations," *International Journal of Production Economics (Elsevier Science),,* pp. vol.75, no.1, p.97-112, 2002.

[20] ISACA, "Cobit5 Executive Overview "Optimise Your Information Systems; Balance Value, Risk and Resources," *ISACA,* p. 4, 2012.

[21] S. von Solms and R. von Solms, Information Security Governance, New York: Springer Science, 2009.

[22] B. De Wit and R. Meyer, Strategy Synthesis: Resolving Strategy Paradoxes to Create Competitive Advantage 2nd ed, London: Thomson , 2005.

[23] W. Van Grembergen and S. De Haes, Implementing Information Technology Governance; Models Practices and Cases, Hershey, United States: IGI 2008.

[24] OECD, "The OECD Principles of Corporate Governance", France, Paris, 2004.

[25] CACG, "CACG Guidelines principles for Corporate Governance. *In the Common Wealth. Towards global competitiveness and economic accountability,*" Commonwealth Association, New Zealand, 1999.

[26] FRC, "Revised Turnbull Guidance," Financial Reporting Council, UK, 2005.

[27] FRC, "THE UK CORPORATE GOVERNANCE CODE," Financial reporting councel, UK, 2010.

[28] King, "King report on Corporate Governance for South Africa," King Committee, South Africa, 2002.

[29] BIS, "Principles for enhancing corporate governance," Bank for International Settlements 2010., Swiss 2010

[30] C. Mallin, Corporate Governance, Third Edition, New York: Oxford University Press, 2010.

[31] D. Hubbard, The Failure of Risk Management, Hoboken New Jersey: John Wiley & Sons, 2009.

[32] G. Westerman and R. Hunter, IT Risk, Turning Business Threats into Competitive Advantage, Boston MA: Hardvard Business School Press, 2007.

[33] COSO, "Enterprise Risk Management Integrated Framework," September 2004.

[34] COSO, "Embracing ERM, Practical Approaches for Getting Started," Committee of Sponsoring Organizations of the Treadway Commission, US 2011

[35] COSO, "Where BoD's currently Stand in executing Their Risk Oversight Responsibilities", US,2011

[36] ITGI, "Information Risks; Who's Business are they?," IT Governance Institute, United States, 2005.

[37] P. Weill and J. Ross, IT Governance, Boston Massachusetts: Harvard Business School Press, 2004.

[38] W. v. Grembergen, Strategies for Information Technology Governance, United States: Idea, 2004.

[39] CGTF, "The Corporate Governance Task Force Report, Information Security Governance: A CALL TO ACTION.," National Cyber Security Summit, US 2004

[40] S. De Haes and W. Van Grembergen, "Practices in IT Governance and Business/IT Alignment," Information System Control Journal, Volume 2, 2008.

[41] H. Kruger and W. Kearney, "A prototype for assessing information security awareness," Science Direct; Computers & Security 25 (289-296), South Africa, 2006.

[42] S. El Aoufi, "Economic Evaluation of Information Security," Vrije University Press, Amsterdam, 2009.

[43] M. Frigo and R. Anderson, "Embracing Enterprise Risk Management: Practical Approaches for Getting Started,"

[44] A. Kankanhalli, T. Hock-Hai, C. Bernard and W. Kwok-Kee, "An integrative study of information systems security effectiveness," *International Journal of Information Management 23,* p. 139–154, 2003.

[45] F. Conner and A. Coviello, "Information Security Governance: A call to action," The Corporate Governance Task Force, United States, 2004.

[46] De Haes, Van Grembergen, "Enterprise governance of IT. Achieving strategic alignment and value," Springer, New York, 2009.

[47] Stackpole, Security Strategy, Boca Raton Florida: Auerbach Publications, 2011.

[48] M. Siponen, "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods," I&O press, 2005.

[49]Hevner, R., "Design Science Research in Information Systems," Management Information Systems Quarterly, Vol. 28, No. 1, pp. 75-105., US, 2004.